Statement of Work
For
Federal Communications Commission –
Emergency Mass Notification and Response System

1.0 INTRODUCTION

The Federal Communications Commission (FCC) is an independent United States government agency, directly responsible to Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia and U.S. possessions.

1.1 Background

The FCC is charged with providing the United States with Operational and Outreach support for State and local public safety and healthcare entities. In addition, the FCC must meet Federal Directives in relation to Continuity of Operations (COOP), Devolution, Pandemic, and Reconstitution Planning, as well as day-to day emergency management. This requires a real time ability to maintain communications and notifications to these entities, as well as licenses, FCC Emergency Response Group members, employees and contractors that support these entities during times of disaster or crisis.

1.2 Acquisition Goal

This statement of work is for an Emergency Mass Notification and Response System, as well as maintenance and support for that system, that will be under the direction of the Office of Managing Director, Associate Managing Director, Administrative Operations.

1.3 Scope of Work

The purpose of this task order is to provide an Emergency Mass Notification and Response System, as well as maintenance and support for that system. An Emergency Mass Notification and Response System are critical to the FCC National Outreach Program which must be able to communicate rapidly with the public safety community, licenses and others from any location. In addition, the FCC requires a notification system for their internal Continuity of Operations (COOP), Devolution, Pandemic, and Reconstitution Plans, as well as the day-to day emergency management efforts.

The system must be a user friendly, "turn-key system" capable of providing geolocation based alerting of FCC licensee points as well as adhoc group alerting of FCC employees; the capability for users to load/import Microsoft Excel data and be able to update alerting groups at user location with minimal steps; and the system should provide a text to voice capability as well as real-time monitoring and be capable of generating reports of status of the alert. Specific requirements include:

- The vendor shall provide a system, maintenance and support that is:
    - Located in at least three geographically diverse facilities to ensure adequate backup should the primary facility go down for any reason.

  - Able to simultaneously activate, FCC and personal E-mail, SMS (texting), voice calls, siren and computer pop-up screens.
  - Web and phone based.

- The vendor shall provide maintenance and support for a system that is capable of:

  - Sending a minimum of 3000 E-mail messages to the FCC email system;
  - Sending a minimum of 3000 computer "Pop-Up" messages to connected FCC government furnished computers;
  - Sending a minimum of 3000 E-mail messages to personal email;
  - Sending a minimum of 1,500 text (SMS) messages to FCC government furnished mobile phones of various vendors
  - Sending a minimum of 3000 messages to personal cell phone numbers;
  - Sending a minimum of 3000 pre-recorded or custom voice messages to FCC telephone numbers;
  - Sending a minimum of 3000 messages to personal telephone numbers;
  - Displaying pre-recorded video or still images on the FCC's closed circuit television network
  - Sending messages to TTY-enabled phones
  - Alerting text messages and audio messages on Cisco VOIP phones.
  - URL re-direction with website interface.
  - Grouping computer systems for group notifications.
  - Notifying up to 3,000 staff via the media sources listed above, within 3-minutes of the FCC activating the system.
  - Continuously notifying staff until each person responds to at least one message on the media source receiving the notification.

- The notification system must provide realtime status, reporting and acknowledgement of receipt for each media source used and store those acknowledgements for future reference and/or reuse by the FCC.
- The notification system must be able to be activated by two-factor authentication from any internet location world-wide.
- The notification system must have a twenty four-seven (24x7) 365 days live technical support that can respond to requests for assistance within 10 minutes.
- Hosting facilities must be able to demonstrate 99.999% availability.
- The vendor must provide semi-annual computer based training and two onsite classroom training at FCC HQ in Washington on the use of the system for up to 25 FCC employees and offer training for significant software changes.
- Pop-up notification must be supported on Windows XP, Windows 7 and Windows 8.
- Communication with pop-up client software must originate from servers located on the FCC's network.
- System must support LDAP and/or AD groups as activation list
- System must be able to export and import system configuration in XML, CSV, or other standard formats.
- System must have the ability to load FCC public safety licensees into a systems database to allow for geographical identification (Geo Mapping), selection and alerting during emergency response situations.

2.0 PERIOD OF PERFORMANCE

The period of performance for this contract is from August 12, 2011 through August 12, 2012, with two (2) additional option years.

2.1 **Place of Performance:** The vendor must provide semi-annual computer based training and one (1) onsite classroom training at mutually agreed dates after contract award on the use of the system for up to 25 FCC employees at the FCC location below:

FCC Headquarters
445 12th Street, SW,
Washington, DC 20554

Equipment, software and hardware will be housed and maintained by the vendor at the facility servicing the FCC.

3.0 ORGANIZATIONAL CONFLICT OF INTEREST

3.1 The provisions of FAR 9.5, titled Organizational and Consultant Conflicts of Interest, govern performance under this contract. As stated at FAR 9.502©, an organizational conflict of interest may result when factors create an actual or potential conflict of interest under this contract, or when the nature of the work to be performed under this contract creates an actual or potential conflict of interest on a future acquisition. In the latter case, some restrictions on the future activities of the contractor may be imposed by the Contracting Officer for the future acquisition.

3.2 FAR 9.505 states that the two underlying principles are (a) preventing the existence of conflicting roles that might bias a contractor's judgment; and (b) preventing unfair competitive advantage. It further states that organizational conflicts of interest may arise in situations covered by FAR 9.505, or the example in FAR 9.508, or in situations not covered by those provisions.

3.3 Under this task order, the contractor may be required to perform services that trigger the concerns and restrictions described in FAR 9.5. Two examples of such situations and related restrictions applicable to performance hereunder, are set forth below.

3.4 Under this task order, the contractor may be required to evaluate offers for products or services. The contractor agrees that it will neither evaluate, nor advise the Government with regard to, its own products or services. In addition, the contractor agrees it will objectively evaluate, and advise the Government concerning, the products or services of its actual or prospective competitors.

4.0 NON-DISCLOSURE

4.1 In the course of performance pursuant to this task order, the contractor will access nonpublic information, including acquisition sensitive information. The contractor agrees that it will not use or disclose any such information unless authorized by the Contracting Officer.

4.2 The contractor further agrees that it will use its best efforts to ensure that its employees and others performing services under this contract will not use or disclose any such information unless authorized by the Contracting Officer. To that end, contractor agrees that its employees and others performing duties under this contract will sign the Certificate of Nondisclosure.

4.3 By agreeing to this task order and/or any amendments, the Contractor acknowledges, understands, and accepts the following:

4.3.1 The Contractor and any Subcontractor(s) shall presume that the FCC computer systems and storage media that the Contractor or Subcontractor access have sensitive information and applications. The Contractor will comply with the contractual security requirements.

4.3.2 Any FCC information, software, applications, computer systems and hardware accessed by the Contractor in the performance of the task order remain the sole property of FCC.

4.3.3 To the extent that any software or applications on the FCC systems are protected by copyright, the Contractor agrees that it will not copy or disclose them without first obtaining the FCC's prior written authorization, which will be provided only where authorized under applicable copyright law.

4.3.4 The Contractor, the Contractor's employees, and any Subcontractor and Subcontractor's employees will access, or be provided access to, the FCC information, software, applications, computer systems and hardware only to the extent necessary, and only for the purpose of, performing the task order. The Contractor will take reasonable steps to ensure that it will allow only those Contractor and Subcontractor employees who need to see the FCC materials to perform the requirements of the task order, to do so. This agreement also applies to any other FCC systems or data to which the Contractor may have access to or be disclosed to the Contractor.

4.3.5 The Contractor will not authorize anyone other than those individuals who require information to perform under the task order to access, disclose, modify, or destroy the information, software or applications on the FCC systems provided or accessed under this task order without the COTR prior written authorization. The Contractor will refer all requests or demands for production of or access to FCC data and systems, including court orders, to the COTR for response.

4.3.6 Except as authorized under this task order, the Contractor and its employees shall not make any copies of any FCC information, including software or applications that are not copyrighted. Any copies made by the Contractor or

Subcontractor shall be identified as FCC property and handled as sensitive information under this non-disclosure agreement.

4.3.7 Except to the extent necessary to perform the task order, any information that the Contractor and its employees learn from and about FCC data and FCC computer systems shall not be recorded and such information, whether recorded or not, shall be handled as sensitive information under this agreement. The Contractor may not use or disclose this data except as the Contractor is permitted to use or disclose FCC sensitive information under the task order and this nondisclosure agreement.

4.3.8 Upon completion or termination of the task order for any reason, the Contractor will immediately deliver all non-public FCC records, data, copies of FCC records and data, software and equipment, and information about FCC data and systems recorded or documented by the Contractor, in its possession or the possession of any Subcontractors to the COTR.

4.3.9 The Contractor will be responsible for the actions of all individuals provided to work for FCC -OMD under this task order.

4.4 Removal from Duty Clause – The Contracting Officer (CO), with input from the COTR and designated FCC Personnel Security Officer, may request that the Contractor immediately remove any contractor personnel from working on the contract should it be determined that individual(s) are unfit to perform on the contract. The FCC will provide the Contractor, in writing, the specific reasons for removal of an individual. The Contractor must comply with these requests.

4.5 Examples of incidents involving misconduct or delinquency are set forth but not limited to the items below:

(a) Violation of the Rules and Regulations Governing Public Buildings and Grounds, 41 Code of Federal Regulations 101-20.3.
(b) Neglect of duty, including sleeping while on duty, unreasonable delays, or failure to carry out assigned tasks, conducting personal affairs during official time, and refusing to cooperate in upholding the integrity of FCC's security program.
(c) Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents or records, or concealment of material facts by willful omissions from official documents or records.
(d) Disorderly conduct, use of abusive or offensive language, quarreling, intimidation by words or actions, or fighting. Also, participating in disruptive activities that interfere with the normal and efficient operations of the Government.
(e) Theft, vandalism, immoral conduct, or any other criminal actions.
(f) Selling, consuming, possession of, or being under the influence of intoxicants, drugs, or substances, which produce similar effects.
(g) Improper use of official authority or credentials.
(h) Unauthorized use of communications equipment or Government property.
(i) Misuse of equipment used in the performance of this contract.
(j) Unauthorized access to areas not required for the performance of the contract.
(k) Unauthorized access to employees' personal property.
(l) Violation of security procedures or regulations.

(m) Prior determination by FCC or other Federal agency that a contractor's employee was unsuitable.
(n) Violation of the Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, and the Taxpayer Browsing Act of 1997.
(o) Unauthorized access to, or disclosure of, agency programmatic or sensitive information, or IRS Tax Return information.
(p) Unauthorized access to FCC's automated information systems.
(q) Unauthorized access of information for personal gain, (including, but not limited to monetary gain) or with malicious intent.

5.0 GOVERNMENT ROLES AND RESPONSIBILITIES

Below are specific roles of government personnel that can direct Contractor resources

5.1 Contracting Officer

The Contracting Officer has responsibility for ensuring the performance of all necessary actions for effective contracting; ensuring compliance with the terms of the contract and safeguarding the interests of the United State in its contractual relationships. Accordingly, the Contracting Officer is the only individual who has the authority to enter into, administer, modify, or terminate this contract. In addition, the Contracting Officer is the only person authorized to approve changes to any of the requirements under this contract, and notwithstanding any provision contained elsewhere in this contract or representation made by any FCC employee, this authority remains solely with the Contracting Officer.

5.2 Contracting Officer Technical Representative (COTR)

The Contracting Officer may designate other Government personnel (known as the Contracting Officer Technical Representative) to act as his or her authorized representative for contract administration functions, including technical direction, that do not involve changes to the scope, performance, price, schedule, or terms and conditions of the contract. The COTR will be named in the order when awarded. Such designation will not contain authority to sign contractual documents, order contract changes, modify contract terms, or create any commitment or liability on the part of the Government different from that set forth in the contract.

5.3 Alternate Contracting Officer Technical Representative (A-COTR)

The Contracting Officer may designate other Government personnel to act as Alternate Contracting Officer Technical Representatives (A-COTR) to assist the COTR and act as the Contracting Officer's authorized representative for contract administration functions, including technical direction, that do not involve changes to the scope, performance, price, schedule, or terms and conditions of the contract. The A-COTR may be named to assist with the administrative functions of the contract. The A-COTR will be named in the order when awarded. Such designation will not contain authority to sign contractual documents, order contract changes, modify contract terms, or create any commitment or liability on the part of the Government different from that set forth in the contract.

6.0 SECTION 508 COMPLIANCE

Compliance with section 508 of the Rehabilitation Act of 1973 (as amended) is mandatory for all

work delivered under the contract. Standards can be viewed at: http://www.section508.gov.

7.0 SUITABILITY AND SECURITY PROCESSING

7.1 General

7.1.1 All task order personnel are subjected to background investigations for the purpose of suitability determinations. Based on their proposed duties, some task order personnel may also be required to have security clearance determinations. No task order personnel may be assigned to work on the task order without a favorable initial review of the OF 306, Declaration for Federal Employment (http://www.opm.gov/forms/pdf_fill/of0306.pdf) or a written waiver from the FCC Security Operations Center (SOC).

7.1.2 Suitability, waiver, and security clearance determination investigations are currently conducted through the FCC SOC (202-418-7884). Individual Contract personnel will be provided with a review process before a final adverse determination is made. The FCC requires that any task order personnel found not suitable, or who has a waiver cancelled, or is denied a security clearance, be removed by the Vendor during the same business day that the determination is made.

7.1.3 If the task order personnel is re-assigned and the new position is determined to require a higher level of risk suitability than the task order personnel currently holds, the individual may be assigned to such position while the determination is reached by the SOC. A new A-600 shall be necessary for the new position.

7.1.4 Task order personnel working as temporary hires (for ninety (90) days or less) must complete and receive a favorable initial review of the OF 306 and complete the task order personnel section of the FCC Form A-600, “FCC SOC Contract Personnel Record ” form. If during the term of their employment they will have access to any FCC network application, they must also complete and sign the FCC Form A-200, “FCC Computer System Application Access Form”.

7.2 At Time of Task Order Award

7.2.1 The FCC SOC must receive the completed, signed OF 306 for each proposed individual member of the contract personnel (i.e., “contract employee”) at the time of task order award. Resumes for all personnel proposed for assignment on the task order shall be provided to the SOC prior to the time of in-take processing (see below, 3.2). **The FCC SOC requires up to five (5) working days (from the date they are received) to process the OF 306 before any employee is allowed to begin work on the contract. A written waiver from the SOC may be obtained in special circumstances.**

All task order personnel, regardless of task description, must complete this form. Without an approved, completed OF 306 on file at the SOC, no Contract personnel may begin work on the Contract. An approved OF 306 is one that has passed initial review by the SOC. During the course of the SOC review of the OF 306, the task order personnel may be interviewed by SOC staff regarding information on their OF 306.

7.2.2 In addition, the Vendor is responsible for submission of completed, signed computer security forms for Contract personnel prior to the individual beginning work on the Contract (See Attachment No. 4, FCC Instruction 1479.2, FCC Computer Security Program Directive

and sample forms.) These forms shall be submitted to the FCC Computer Security Office.

7.2.3 The COTR shall begin processing their Section B of the FCC task order FCC SOC Contract Personnel Record form (FCC Form A-600) prior to Contractor award notification. This form, with the COTR and CO portions completed, will be distributed at the time of task order award and the Contractor must submit the completed A-600 forms for all Contract personnel to the SOC within ten (10) working days of contract award execution.

7.2.4 The Office of Personnel Management (OPM) will issue a Certificate of Investigation (CIN) following the appropriate background investigation. The SOC notifies the CO and COTR and task order personnel who have received a favorable adjudication so they may receive their permanent access credential.

7.3 **Identity Proofing, Registration and Checkout Requirements**

Contractor shall comply with the Identity Proofing, Registration, and Checkout Requirements.

8.0 Additional Terms, Conditions, Obligations Under this Order

8.1 **Invoices**

Invoices may be submitted via email to: FO-Einvoices@fcc.gov. In addition, copies of the emailed invoices shall also be sent to the CO and COTR. Or, they may be submitted in an original and two copies to: FCC Travel Operations Group, Room #1A761, 12th Street, S.W., Washington, DC 20554. Requirements for proper invoices are set forth in FAR 52.212-4(g). The Commission will return all improper invoices without action.